EXHIBIT 1

FILED
Williamson Co. Circuit Court
1st Judicial Circuit
Date: 6/15/2023 2:34 PM
Justin Maze

IN THE CIRCUIT COURT
FIRST JUDICIAL CIRCUIT
WILLIAMSON COUNTY, ILLINOIS

JOHN DOE, Individually, and on behalf of all others similarly situated,	2023LA55
Plaintiff	Case No. _____
v.	CLASS ACTION
SOUTHERN ILLINOIS HEALTHCARE ENTERPRISES, INC., SOUTHERN ILLINOIS HOSPITAL SERVICES, and SOUTHERN ILLINOIS MEDICAL SERVICES, NFP,	JURY TRIAL DEMANDED
Defendants.	

CLASS ACTION COMPLAINT

Plaintiff, JOHN DOE, Individually, and on behalf of all others similarly situated (hereinafter "Plaintiff") brings this Class Action Complaint against Defendants, SOUTHERN ILLINOIS HEALTHCARE ENTERPRISES, INC., SOUTHERN ILLINOIS HOSPITAL SERVICES, and SOUTHERN ILLINOIS MEDICAL SERVICES, NFP collectively d/b/a SOUTHERN ILLINOIS HEALTHCARE (hereinafter "SIH" or "Defendants"), and alleges, upon personal knowledge as to their own actions, and upon information and belief as to all other matters, as follows.

INTRODUCTION

1. Plaintiff brings this class action to address Defendants' outrageous, illegal, and widespread practice of disclosing the confidential Personally Identifying Information[1] ("PII")

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's

EXHIBIT 1

and/or Protected Health Information[2] ("PHI") (collectively referred to as "Private Information") of Plaintiff and the proposed Class Members to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook" or "Meta"), Google, LLC ("Google"), and others. ("the Disclosure").

2. Information about a person's physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of medical information can have serious consequences, including discrimination in the workplace and denial of insurance coverage. If people do not trust that their medical information will be kept private, they may be less likely to seek medical treatment, which can lead to more serious health problems down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than the person's medical provider is necessary to maintain public trust in the healthcare system.

3. Recognizing these facts, and in order to implement requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the United States Department of Health and Human Services ("HHS") has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how health care providers must safeguard and protect Private Information. Under the HIPAA Privacy Rule, no

license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). SIH is clearly a "covered entity" and some of the data compromised in the Disclosure that this action arises out of is "protected health information," subject to HIPAA.

health care provider can disclose a person's personally identifiable protected health information to a third party without express written authorization.

4. According to Defendants, "Southern Illinois Healthcare (SIH) is a not-for-profit health system serving the southernmost counties of Illinois with four hospitals, a comprehensive cancer center, Level II Trauma Center and more than 30 outpatient and specialty practices. Based in Carbondale, Ill., SIH is the region's largest private employer with 4,000 employees . . . ."[3]

5. Defendants encourage their patients to use their website, https://www.sih.net/, (the "Website") and their various web-based tools and services, allowing patients to search for physicians, locate healthcare facilities, learn about specific health conditions and treatment options, and more (collectively referred to as the "Online Platforms").

6. Despite its unique position as a massive and trusted healthcare provider, SIH knowingly configured and implemented devices known as "pixels" to collect and transmit patient information, including information communicated by patients through Defendants' sensitive and presumptively confidential Online Platforms, to third parties.

7. When Plaintiff and Class Members used Defendants' Website and Online Platforms, they thought were communicating exclusively with their trusted healthcare provider. Unbeknownst to them, Defendants surreptitiously forced Plaintiff and Class Members to transmit intimate details about their medical treatment to third parties through the use of pixels, which Defendants had placed on their Website and Online Platforms.

8. A pixel (also referred to as a "tracker" or "tracking technology") is a snippet of code that tracks information about website visitors and their interactions.[4] When a person visits a

[3] About Us, SIH, https://www.sih.net/about-us (last visited June 12, 2023).
[4] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).

website with an embedded pixel, the pixel tracks "events" (i.e., user interactions with the site), such as pages viewed, buttons clicked, and information submitted through the site.[5] As the visitor interacts with the website, the pixel transmits the event information back to the website server and to third parties, who then use that data for their own products and services.[6]

9. Among the pixels Defendants embedded into their Website is the Facebook Pixel (also referred to as the "Meta Pixel" or "Pixel"). By default, the Meta Pixel tracks information about a visitor's device, including their IP address, and the pages viewed.[7] When configured, the Meta Pixel can track much more, including a visitor's search terms, button clicks, and form submissions.[8] Additionally, the Meta Pixel can link a visitor's website interactions with an individual's unique and persistent Facebook ID ("FID"), allowing a user's health information to be linked with their Facebook profile.[9]

10. Operating as designed and as implemented by Defendant, the Meta Pixel allowed Defendants to unlawfully disclose Plaintiff and Class Members' Private Health Information to Facebook. By installing the Meta Pixel on their Website, Defendants effectively planted a bug on Plaintiffs' and Class Members' web browsers and compelled them to disclose their Private Information and confidential communications to Facebook, without their authorization or knowledge.

---

[5] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).
[6] *Id.*
[7] *See* Get Started, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/get-started (last visited May 22, 2023).
[8] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).
[9] The Meta Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites about the user, enabling the websites to personalize the user experience." What are Cookies?, https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).

11. Facebook encourages and recommends the use of its Conversions Application Programming Interface ("CAPI") alongside use of the Meta Pixel.[10]

12. Unlike the Meta Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook in addition to the website owner, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interaction, including Private Information, records and stores that information on the website owner's servers, and then transmits the data to Facebook from the website owner's servers.[11, 12]

13. Indeed, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[13]

14. Because CAPI is located on the website owner's servers and is not a bug planted onto the website user's browser, it allows website owners like Defendants to circumvent any ad blockers or other denials of consent by the website user that would have prevented the Meta Pixel from sending website users' Private Information to Facebook directly. Thus, CAPI allows website owners to spy on their visitors' activities without detection or consent, and then transmit information about those interactions to Facebook, without the visitor's knowledge.

---

[10] "CAPI works with your Meta Pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* Samir El Kamouny, How to Implement Facebook Conversions API (In Shopify), FETCH & FUNNEL https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited Jan. 25, 2023).

[11] What is the Facebook Conversion API and How to Use It, REVEALBOT BLOG, https://revealbot.com/blog/facebook-conversions-api/ (last updated May 20, 2022).

[12] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel…. This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." Conversions API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/conversions-api (last visited May 15, 2023).

[13] About Conversions API, META FOR DEVELOPERS, https://www.facebook.com/business/help/2041148702652965 (last visited May 15, 2023).

15. Defendants utilized data from these trackers to market its services and bolster its profits. The data collected by Meta Pixel and CAPI allows website owners like Defendant to build profiles for specific individuals for the purposes of retargeting and future marketing. Facebook also uses this data to create targeted advertisements based on the medical conditions and other information disclosed to Defendant.

16. The data collected and sent to Facebook via Defendant's use of the Meta Pixel and CAPI includes Plaintiff and Class Members' confidential communications and interactions with Defendant's website, including, for example, the contents of their search queries, the parameters of their doctor searches, the pages they visited, and the buttons that they clicked.

17. Such information allows a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. Facebook, in turn, sells Plaintiff's and Class Members' Private Information to third-party marketers, who then geotarget Plaintiff's and Class Members' Facebook pages based on communications obtained via Meta Pixel and CAPI. Facebook and any third-party purchasers of Plaintiff's and Class Members' Private Information also could reasonably infer from the data that a specific patient was being treated for a specific type of medical condition, such as cancer, pregnancy, dementia, or HIV.

18. In addition to the Facebook tracker and CAPI, Defendants installed other tracking technology, including Google Analytics, Facebook Events, ShareThis, Mailchimp for WeeCommerce, and CallTrk. On information and belief, these trackers operate similarly to the Meta Pixel and transmit a website user's Private Information to other third parties.

19. Healthcare patients simply do not anticipate that their trusted healthcare provider will send Personal Health Information or other confidential medical information collected via its

webpages to a hidden third party—let alone Facebook, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue—without the patients' consent.

20. Neither Plaintiff nor any Class Member signed a written authorization permitting Defendants to send their Private Information to Facebook, Google, ShareThis, Mailchimp, and CallRail, or any other third parties uninvolved in their treatment.

21. Despite willfully and intentionally incorporating tracking technology, including the Meta Pixel, potentially CAPI and other tracking technology, into its Website and servers, SIH has never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications and Private Information with third parties including Facebook, and possibly Google, ShareThis, Mailchimp, CallRail and others.

22. Plaintiff and Class Members were unaware that their Private Information was being surreptitiously transmitted to Facebook and other third parties as they communicated their confidential PHI with their healthcare provider via the Website.

23. Defendants further made express and implied promises to protect Plaintiff's and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchanged with Defendant.

24. Defendants owed common law, statutory, and regulatory duties to keep Plaintiff's and Class Members' communications and Private Information safe, secure, and confidential.

25. Upon information and belief, SIH utilized the Meta Pixel and other tracker data to improve and to save costs on its marketing campaigns, improve its data analytics, attract new patients, and generate sales.

26. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties to those

individuals to protect and to safeguard that information from unauthorized disclosure.

27. Defendants breached their statutory and common law obligations to Plaintiff and Class Members by, *inter alia*,: (i) failing to adequately review their marketing programs and web-based technology to ensure the hospital Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) aiding, agreeing, and conspiring with third parties to intercept communications sent and received by Plaintiff and Class Members; (iv) failing to obtain the written consent of Plaintiff and Class Members to disclose their Private Information to Facebook and others; (v) failing to protect Private Information and take steps to block the transmission of Plaintiff's and Class Members' Private Information through the use of Meta Pixel and other tracking technology; (vi) failing to warn Plaintiff and Class Members; and (vii) otherwise failing to design and monitor their Website to maintain the confidentiality and integrity of patient Private Information.

28. Plaintiffs seek to remedy these harms and bring causes of action for (I) Negligence, (II) Invasion of Privacy, (III) Breach of Implied Contract, (IV) Unjust Enrichment; (V) Breach of Fiduciary Duty, and (VI) Violation of the Illinois Consumer Fraud and Deceptive Practices Act (CFDPA), 815 Ill. Comp. Stat. § 505/1 *et seq*.

PARTIES

29. Plaintiff, John Doe, is a natural person and a resident and citizen of Illinois, where he intends to remain, with a principal residence in Williamson County. He has been a patient of SIH for approximately twenty years, and he is a victim of Defendants' unauthorized Disclosure of Private Information.

30. Defendants (Southern Illinois Healthcare Enterprises, Inc., Southern Illinois Hospital Services, and Southern Illinois Medical Services, NFP hereinafter referred to as "SIH" or

"Defendants") are non-profit corporations doing business collectively under the name "Southern Illinois Healthcare." They are each organized and exist under the laws of the State of Illinois, and they share a principal place of business at 1239 East Main Street, Carbondale, Illinois 62901, in Jackson County, Illinois

JURISDICTION AND VENUE

31. This Court has jurisdiction over the subject matter of this action by virtue of the Illinois Constitution, article 6, section 9, which provides that "Circuit Courts shall have original jurisdiction in all matters justiciable," unless the matter falls into the limited original jurisdiction of the Illinois Supreme Court.

32. This Court has personal jurisdiction over Defendants because Defendants have engaged in the "transaction of any business within this State." 735 Ill. Comp. Stat. Ann. 5/2-209.

33. Venue is proper because all Defendants reside, have a principal place of business and do business in Williamson County, Illinois, and under the Illinois Consumer Fraud and Deceptive Practices Act, 815 Ill. Comp. Stat. Ann. 505/1 *et seq.*, an "action may be commenced in the county in which the person against whom it is brought resides, has his principal place of business, or is doing business, or in the county were the transaction or any substantial portion thereof occurred." *Id.* at 505/10a; *see also* 735 Ill. Comp. Stat. Ann. 5/2-101.

COMMON FACTUAL ALLEGATIONS

A. Background

34. SIH headquartered in Carbondale, Illinois, and is the region's largest healthcare provider. It employs over 4000 people and supplying 378 of the region's hospital beds. [14] Memorial Hospital of Carbondale, SIH's flagship hospital, operates forty-five specialty practices, including

[14] About Us, SIH, https://www.sih.net/about-us (last visited June 9, 2023).

the region's only pediatric unit, and is a "regional referral center for the 16-county Southern Illinois region."[15] In addition to Memorial Hospital, operates three other area hospitals (Herrin Hospital, St. Joseph Memorial, and Harrisburg Medical Center)[16] and nearly sixty other general practice and specialty clinics.[17]

35. SIH serves many of its patients via its Online Platforms, which it encourages patients to use to find healthcare services and providers, access information about specific health conditions, request appointments, and more. Defendants promote the convenience and comprehensive functionality of these Online Platforms.

36. Defendants purposely installed the Meta Pixel and trackers on its Website, to gather data about Plaintiff and Class Members for the purpose of advertising and increasing sales. In doing so, Defendants used Plaintiff and Class Members' Private Information for marketing purposes without their consent, and further, shared that Private Information with Facebook and other third parties.

37. To better understand Defendants' unlawful data-sharing practices, a brief discussion of basic web design and tracking tools follows.

i. Facebook's Business Tools and the Meta Pixel

38. As Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[18]

39. In conjunction with its advertising business, Facebook encourages and promotes

[15] *Id.*
[16] *Id.*
[17] Locations, SIH, https://www.sih.net/locations (last visited June 12, 2023).
[18] Meta Reports Fourth Quarter and Full Year 2021 Results, FACEBOOK https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Nov. 14, 2022).

entities and website owners, such as Defendant, to utilizes its "Business Tools" to gather, identify, target, and market products and services to individuals.

40. Facebook's Business Tools, including the Meta Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

41. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, the webpage's Universal Resource Locator ("URL"), as well as metadata, button clicks, and other information.[19] Businesses that want to target customers and advertise their services, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[20]

42. One such Business Tool is the Meta Pixel, a tool that "tracks the people and type of actions they take" while visiting a website.[21]

43. The Meta Pixel's primary purpose is for marketing and ad targeting and sales generation.[22] Facebook's website informs companies that "[t]he Meta Pixel is a piece of code that you put on your website that allows you to measure the effectiveness of your advertising by understanding the actions people take on your website."[23]

---

[19] Specifications for Facebook Pixel Standard Events, META, https://www.facebook.com/business/help/402791146561655 (last visited Jan. 31, 2023); *see also* Facebook Pixel, Accurate Event Tracking, Advanced, META FOR DEVELOPERS; https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* Best Practices for Facebook Pixel Setup, META https://www.facebook.com/business/help/218844828315224; App Events API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Jan. 31, 2023).

[20] About Standard and Custom Website Events, META, https://www.facebook.com/business/help/964258670337005; *see also* Facebook, App Events API, *supra*.

[21] Retargeting, META, https://www.facebook.com/business/goals/retargeting.

[22] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).

[23] About Meta Pixel, META, https://www.facebook.com/business/help/742478679120153 (last accessed Mar. 19, 2023).

44. Facebook boasts to its prospective users that the Meta Pixel can be used to:

- **Make sure your ads are shown to the right people.** Find new customers, or people who have visited a specific page or taken a desired action on your website.

- **Drive more sales**. Set up automatic bidding to reach people who are more likely to take an action you care about, like making a purchase.

- **Measure the results of your ads.** Better understand the impact of your ads by measuring what happens when people see them.[24]

45. When a user accesses a webpage that is hosting the Meta Pixel, the communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook, traveling from directly the user's browser to Facebook's server.

46. According to Facebook, the Meta Pixel can collect the following data.

> **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page location, document, referrer and ***person using the website.*** (emphasis added).
>
> **Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.
>
> **Button Click Data** – Includes any buttons clicked by site visitors, the labels those buttons and any pages visited as a result of the button clicks.
>
> **Optional Values** – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.
>
> **Form Field Names** – Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values unless you include them as part of Advanced Matching or optional values.[25]

47. Notably, this transmission only occurs on webpages that contain the Meta Pixel. A

[24] About Meta Pixel, META, https://www.facebook.com/business/help/742478679120153 (last accessed Mar. 19, 2023).
[25] Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).

website owner could configure its website to use the Pixel on pages that don't implicate patient privacy (such as the homepage) and disable it on pages that do implicate patient privacy (such as the Website's physician-search feature).

48. Not only website owners use and benefit from data gathered by the Meta Pixel: Facebook likewise benefits from and uses the data to target users and serve targeted ads.

ii. Defendants' method of transmitting Plaintiff's and Class Members' Private Information via the Meta Pixel and/or Conversions API i.e., the Interplay between HTTP Requests and Responses, Source Code, and the Meta Pixel

49. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. Each "client device" (such as computer, tablet, or smart phone) accesses web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

50. Every website is hosted by a computer "server" that holds the website's contents and through which the website owner exchanges files or communications with Internet users' client devices via their web browsers.

51. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies.[26]

52. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), they also send the host server data, which is embedded inside the URL and can include cookies.

[26]"Cookies are small files of information that a web server generates and sends to a web browser . . . . Cookies help inform websites about the user, enabling the websites to personalize the user experience." https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).

53. When an individual visits a website, their web browser sends an HTTP Request to the entity's servers that essentially asks the website to retrieve certain information (such as Defendants' physician-search page). The entity's servers send the HTTP Response, which contains the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate a website.

54. Every website is comprised of Markup and "Source Code." Source Code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

55. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user.

56. The implementation of the Meta Pixel is source code that acted much like a traditional wiretap, intercepting and transmitting communications between the website user and the website host and sending those communications to a third party.

57. Separate from Meta Pixel, Facebook and other website owners can place third-party cookies in the web browsers of users logged into their websites or services. These cookies can uniquely identify the user so the cookie owner can track the user as she moves around the internet—whether on the cookie owner's website or not. Facebook uses this type of third-party cookie when Facebook account holders use the Facebook app or website. As a result, when a Facebook account holder uses a website with the Meta Pixel, the account holder's unique Facebook ID is sent to Facebook, along with the intercepted communication, allowing Facebook to identify the patient associated with the Private Information it has intercepted.

58. With substantial work and technical know-how, internet users can sometimes

circumvent this browser-based wiretap technology. To counteract this, third parties bent on gathering data and Private Information implement workarounds that are difficult to detect or evade. Facebook's workaround is its Conversions API tool ("CAPI"), which is particularly effective because the data transmitted via this tool does not rely on the website visitor's web browsers. Rather, the information travels directly from the entity's server to Facebook's server.

59. CAPI "is designed to create a direct connection between [web hosts'] marketing data and [Facebook]."[27] Thus, the entity receives and stores its communications with patients on its server before CAPI collects and sends those communications—and the Private Information contained therein—to Facebook.

60. Notably, client devices do not have access to host servers and thus cannot prevent (or even detect) this additional transmission of information to Facebook.

61. While there is no way to confirm with certainty that a website owner is using CAPI without accessing the host server, Facebook instructs companies like Defendants to "[u]se the Conversions API in addition to the Meta Pixel, and share the same events using both tools," because such a "redundant event setup" allows the entity "to share website events [with Facebook] that the pixel may lose."[28] Thus, if an entity implemented the Meta Pixel in in accordance with Facebook's documentation, it is also reasonable to infer that it implemented the CAPI tool on its Website.

62. The third parties who receive data through pixels and other tracking technology do not provide any substantive content on the host website. That is, Facebook and others like it are not providing anything to the user relating to the user's communications. Instead, these third

[27] About Conversions API, META, https://www.facebook.com/business/help/2041148702652965 (last visited May 15, 2023).
[28] *See* Best Practices for Conversions API, META, https://www.facebook.com/business/help/308855623839366 (last visited May 15, 2023).

parties are typically procured to track user data and communications only to serve the marketing purposes of the website owner (i.e., to bolster profits).

63. Accordingly, without any knowledge, authorization, or action by a user, website owners like Defendants can use its source code to commandeer its patients' computing devices, causing the device's web browser to simultaneously invisibly re-direct the patients' communications to Facebook and possibly other hidden third parties.

64. In this case, Defendants employed the Meta Pixel, and potentially CAPI, to intercept, duplicate, and re-direct Plaintiff's and Class Members' Private Information to Facebook, simultaneously, invisibly, and without the patient's knowledge.

65. SIH also employed other trackers, including Google Analytics, Facebook Events, ShareThis, Mailchimp for WeeCommerce, and CallTrk, which, on information and belief, likewise transmitted Plaintiff's and the Class Members' Private Information to third parties without Plaintiff's and Class Members' knowledge or authorization.

iii. Defendants Violated its own Privacy Policies

66. SIH maintains and is covered under its Privacy Policy, published on Defendants' Website.[29]

67. Defendants' Privacy Policy provides, "[t]his Notice describes the privacy practices of Southern Illinois Healthcare."

68. On information and belief, Defendants do not maintain a separate Website privacy policy.

69. In its Privacy Policy, SIH acknowledges that it is "required by law to maintain the privacy and security of your individually identifiable health information **Protected Health**

[29] *See* Privacy Policy, SIH, https://www.sih.net/privacy-policy (last visited June 12, 2023), **attached as Exhibit A.**

Information, or, **("PHI")**, and to provide you with this Notice of our legal duties and privacy practices with respect to your Protected Health Information."[30]

70. SIH further states in its policy the limited purposes for which it may use or disclose PHI without patient authorization, such as providing medical treatment and obtaining payment. Notably, these purposes do not include marketing, advertising, and web services.[31]

71. SIH represents and promises that it will not "use or share" PHI "[f]or any purpose other than the ones described," unless "you grant us your written authorization."[32]

72. Additionally, SIH represents and promises in its Privacy Policy that "**[w]e must get your written permission prior to using your protected health information to send you any marketing materials.**"[33]

73. Despite these representations, Defendants have, in fact, used and shared Plaintiff's and Class Member's Private Information with unauthorized third parties, including Facebook, without the knowledge of Plaintiff and Class Members and without their written authorization.

74. Defendants disclosed Plaintiff's and Class Members' Private Information and confidential communications to Facebook and others by collecting data on Website user interactions and sending that data to Facebook. For example, when a patient visits Defendants' Website and clicks "Cancer Care" under Defendants' "Services & Treatments" page, the individual's browser sends a request to Defendants' server requesting that it load the webpage. Then, Meta Pixel sends secret instructions back to the individual's browser, causing it to imperceptibly record the patient's communication with SIH and transmit that record to Facebook's servers alongside personally identifying information, such as the patient's IP address. In this way,

[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] *Id.*

Defendants disclosed Plaintiff's and Class Members' Private Information to Facebook.

75. Facebook takes the user data received from companies like Defendants and uses it to build web user profiles and "audiences" to improve its own marketing and targeting services and to advertise products to specific users and audiences.

76. Google and other companies process this data in a similar manner and use it to connect the information to build marketing and other data profiles on particular individuals and audiences.

77. By using and sharing Plaintiff's and Class Members Private Information for purposes not disclosed in the policy, Defendants violated their own Privacy Policy.

78. Defendants used and disclosed Plaintiff's and Class Members' Private Information for the purpose of marketing their services and increasing their profits.

79. By using Plaintiff's and Class Members' Private Information for marketing purposes, Defendants violated their Privacy Policy.

80. On information and belief, Defendants also shared, traded, or sold Plaintiff's and Class Members' Private Information to Facebook, and potentially other third parties, in exchange for improved targeting and marketing services. This too was an unauthorized and undisclosed use of Plaintiff and Class Members' Private Information.

81. Additionally, Defendants misrepresented that they would preserve the security and privacy of Plaintiff's and Class Members' Private Information. In fact, Defendants had knowingly shared Plaintiff and Class Members Private Information with Facebook, Google, and likely other third parties.

82. Defendants could have chosen not to use the Meta Pixel and other tracking technology, or they could have configured their trackers to limit the information that it

communicated to third parties, but they did not. Instead, they intentionally took advantage of these trackers' features and functions, resulting in the Disclosure of Plaintiffs' and Class Members' Private Information.

83. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendants to use and disclose their Private Information for marketing purposes or to intercept their confidential communications. Plaintiff was never provided with any written notice that Defendants disclose their patients' Protected Health Information, nor were they provided any means of opting out of such disclosures. Defendants nonetheless knowingly disclosed Plaintiff's Protected Health Information to Facebook and possibly other unauthorized entities.

84. Plaintiffs and Class Members relied on Defendants' promise to keep their Private Information confidential and securely maintained, to use this information for legitimate healthcare purposes only, and to make only authorized disclosures of this information.

85. By law, Plaintiffs and the Class Members are entitled to privacy in their Protected Health Information and confidential communications. SIH deprived Plaintiff and Class Members of their privacy rights when it (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiff's and Class Members' confidential communications, Personally Identifiable Information, and Protected Health Information; (2) disclosed patients' Private Information to unauthorized, third-party eavesdroppers, including Facebook and possibly others; and (3) undertook this pattern of conduct without notifying Plaintiff and Class Members and without obtaining their express written consent.

B. Plaintiffs' Experiences

Plaintiff John Doe's Experience

86. Plaintiff John Doe has been a patient of SIH for approximately twenty years. He

has received healthcare services from SIH and physicians in SIH's network. He relied on Defendants' Online Platforms to search for doctors and schedule appointments.

87. Plaintiff Mr. Doe accessed Defendants' Online Platforms at Defendants' direction and encouragement. Mr. Doe reasonably expected that his online communications with SIH were confidential, solely between himself and SIH, and that, as such, those communications would not be transmitted to or intercepted by a third party.

88. Plaintiff Mr. Doe provided his Private Information to Defendants and trusted that the information would be safeguarded according to SIH's privacy policies and the law.

89. As described herein, by use of the Meta Pixel and tracking technology, SIH sent Mr. Doe's Private Information to Facebook and possibly others when he used Defendants' Online Platforms to communicate private health information to SIH.

90. Pursuant to the process described herein, SIH assisted Facebook and possibly others with intercepting Mr. Doe's confidential communications, including those that contained PII and PHI. SIH facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

91. By failing to receive the requisite consent and unlawfully disclosing Plaintiff's Private Information, SIH breached its duty and commitment to protect and keep confidential Plaintiff's personal health information.

C. Investigations and Reports Reveal the Meta Pixel's Impermissible Collection of PHI

92. In June 2020, after promising users that app developers would not have access to data if users were not active in the prior ninety days, Facebook revealed that it still enabled third-party developers to access this data.[34] This failure to protect users' data enabled thousands of

[34] Kurt Wagner & Bloomberg, Facebook Admits Another Blunder with User Data, FORTUNE (July 1, 2020 at 6:30 p.m.) https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/.

developers to see data on inactive users' accounts if those users were Facebook friends with someone who was an active user.

93. On February 18, 2021, the New York State Department of Financial Services released a report detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that "[t]he information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective . . . at preventing the receipt of sensitive data."[35]

94. The New York State Department of Financial Service's concern about Facebook's cavalier treatment of private medical data was not misplaced. In June 2022, the FTC finalized a different settlement involving Facebook's monetizing of sensitive medical data. In that case, the more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing their data with Facebook.[36] When a user was having her period or informed the app of her intention to get pregnant, Flo would tell Facebook, which could then use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about secretly sharing their data with Facebook, as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC reported that Flo "took no action to limit what these companies could do with

[35] New York State Department of Financial Services, REPORT ON INVESTIGATION OF FACEBOOK INC. DATA PRIVACY CONCERNS, (Feb. 18, 2021) https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf.

[36] Justin Sherman, Your Health Data Might Be for Sale, SLATE (June 22, 2022 at 5:50 a.m.) https://slate.com/technology/2022/06/health-data-brokers-privacy.html.

users' information."[37]

95. More recently, Facebook employees admitted to lax protections for sensitive user data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that "[w]e do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"[38]

96. Furthermore, in June 2022, an investigation by The Markup[39] revealed that the Meta Pixel was embedded on the websites of 33 of the top 100 hospitals in the nation.[40] On those hospital websites, the Meta Pixel collects and sends Facebook a "packet of data," including sensitive personal health information, whenever a user interacts with the website, for example, by clicking a button to schedule a doctor's appointment.[41] The data is connected to an IP address, which is "an identifier that's like a computer's mailing address and can generally be linked to a specific individual or household—creating an intimate receipt of the appointment request for Facebook."[42]

97. During its investigation, The Markup found that Facebook's purported "filtering" failed to discard even the most obvious forms of sexual health information. Worse, the article found that the data that the Meta Pixel was sending Facebook from hospital websites not only included details such as patients' medications, descriptions of their allergic reactions, details about

[37] *Id.*
[38] Lorenzo Franceschi-Bicchierai, Facebook Doesn't Know What It Does with Your Data, or Where It Goes: Leaked Document, VICE (April 26, 2022) https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes.
[39] The Markup is a nonprofit newsroom that investigates how powerful institutions are using technology to change our society. *See* www.themarkup.org/about (last accessed Mar. 19, 2023).
[40] Todd Feathers, Simon Fondrie-Teitler, Angie Waller, & Surya Mattu, Facebook Is Receiving Sensitive Medical Information from Hospital Websites, THE MARKUP (June 16, 2022 6:00 a.m.) https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.
[41] *Id.*
[42] *Id.*

their upcoming doctor's appointments, but also included patients' names, addresses, email addresses, and phone numbers.[43]

98. In addition to the 33 hospitals identified by The Markup that had installed the Meta Pixel on their websites, The Markup identified seven health systems that had installed the Meta Pixel inside their password-protected patient portals.[44]

99. David Holtzman, health privacy consultant and former senior privacy adviser in the U.S. Department of Health and Human Services' Office for Civil Rights, stated he was "deeply troubled" by what the hospitals capturing and sharing patient data in this way.[45]

D. Defendants Violated HIPAA Standards

100. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-public medical information (PHI) about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[46]

101. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

102. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at

[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

a certain clinic, then this information would be PHI.[47]

103. In its guidance for Marketing, the Department further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list. (Emphasis added).[48]

104. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technology.[49]

105. According to the Bulletin, "HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information."[50]

106. Citing The Markup's June 2022 article, the Bulletin expressly notes:

> Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors. **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules**. For example, disclosures of PHI to tracking technology vendors or marketing purposes, without

---

[47] U.S. Department of Health and Human Services, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, (Nov. 26, 2012) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

[48] U.S. Department of Health and Human Services, Marketing, (Dec. 3, 2002) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.

[49] *See* U.S. Department of Health and Human Services, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/hipaa-online-tracking/index.html.

[50] *Id.*

> individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.
>
> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule. [51]

107. In other words, HHS has expressly stated that Defendants' conduct of implementing the Meta Pixel is a violation of HIPAA Rules.

E. Defendants Violated Industry Standards

108. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

109. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications, which are applicable to SIH and its physicians.

110. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care . . . . Patient privacy encompasses a number of aspects, including . . . personal data (informational privacy).

111. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent

[51] *Id.* (emphasis in original) (internal citations omitted).

> undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (a) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

112. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically . . . must . . . release patient information only in keeping ethics guidelines for confidentiality.

F. Plaintiff's and Class Members' Expectation of Privacy

113. At all times when Plaintiff and Class Members provided their Private Information to Defendants, they all had a reasonable expectation that the information would remain private and that Defendants would not share the Private Information with third parties for commercial marketing and sales purposes.

G. IP Addresses are Personally Identifiable Information

114. Using Meta Pixel and other tracking technologies, Defendants disclosed Plaintiff's and Class Members' IP addresses to Facebook or otherwise assisted Facebook with intercepting Plaintiff and Class Members' IP addresses.

115. An IP address is a number that identifies the address of a device connected to the Internet.

116. IP addresses are used to identify and route communications on the Internet.

117. IP addresses of individual Internet users are used by Internet service providers, Websites, and third-party tracking companies to facilitate and track Internet communications.

118. Facebook tracks every IP address ever associated with a Facebook user.

119. Facebook tracks IP addresses for use of targeting individual homes and their

occupants with advertising.

120. Under HIPAA, an IP address is Personally Identifiable Information:

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).

- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See also*, 45 C.F.R. § 164.514(b)(2)(i)(O).

121. Consequently, by disclosing IP addresses, Defendants' business practices violated HIPAA, industry privacy standards, and Plaintiff and Class Members reasonable expectation of privacy.

H. Defendants Benefitted from and Were Enriched by Using the Pixel to Make Unauthorized Disclosures

122. The sole purpose for Defendants' use of the Meta Pixel and other tracking technology was marketing their services and increasing their profits.

123. In exchange for disclosing the Private Information of their patients, Defendants are compensated by Facebook and potentially other third parties in the form of enhanced advertising services and more cost-efficient marketing on its platform.

124. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions. Upon information and belief, as part of their marketing campaign, Defendants re-targeted patients and potential patients.

125. By utilizing the Meta Pixel and other trackers, the cost of advertising and retargeting was reduced, thereby benefiting Defendant.

I. Plaintiff's and Class Members' Private Information Had Financial Value

126. Plaintiff's data and Private Information has economic value. Facebook regularly

uses data that it acquires to create Core and Custom Audiences, as well as Lookalike Audiences and then sells that information to advertising clients.

127. Data harvesting is one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is due to increase; estimates for 2022 are as high as $434 per user, for a total of more than $200 billion industry wide.

128. In particular, the value of health data is well-known due to the media's extensive reporting on the subject. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry." Therein, Time Magazine described the extensive market for health data and observed that the health data market is both lucrative and a significant risk to privacy.[52]

129. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[53]

TOLLING, CONCEALMENT, AND ESTOPPEL

130. The applicable statutes of limitation have been tolled as a result of SIH's knowing and active concealment and denial of the facts alleged herein.

131. SIH seamlessly incorporated Meta Pixel and other trackers into its Website and Online Platforms while providing users with no indication that their Website usage was being

[52] *See* Adam Tanner, How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry, TIME, (Jan. 9, 2017 at 9:00 a.m.) https://time.com/4588104/medical-data-industry/.
[53] *See* Christina Farr, Hospital Execs Say They are Getting Flooded with Requests for Your Health Data, CNBC, (Dec. 18, 2019 at 8:27 a.m.) https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.

tracked and transmitted to third parties. SIH knew that its Website incorporated Meta Pixel and other trackers, yet it failed to disclose to Plaintiff and Class Members that their sensitive medical information would be intercepted, collected, used by, and disclosed to Facebook, and likely other third parties, including Google, ShareThis, Mailchimp, and CallRail.

132. Plaintiff and Class Members could not with due diligence have discovered the full scope of SIH's conduct, because there were no disclosures or other indication that they were interacting with websites employing Meta Pixel or any other tracking technology.

133. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. SIH's illegal interception and disclosure of Plaintiff's Private Information has continued unabated through the present. Moreover, SIH was under a duty to disclose the nature and significance of their data collection practices but did not do so. SIH is therefore estopped from relying on any statute of limitations defenses.

CLASS ALLEGATIONS

134. Plaintiff brings this statewide class action on behalf of himself and on behalf of other similarly situated persons.

135. The statewide Class that Plaintiff seeks to represent is defined as follows:

> **All Illinois citizens whose Private Information was disclosed by Defendants to third parties through the Meta Pixel and related technology without authorization.**

136. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers, and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state, or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards,

sections, groups, counsels, and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

137. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

138. Numerosity: Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds or thousands of individuals whose Private Information may have been improperly accessed in the Disclosure, and each Class is apparently identifiable within Defendants' records.

139. Commonality: Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include

a. whether and to what extent Defendants had a duty to protect Plaintiff's and Class Members' Private Information;

b. whether Defendants had duties not to disclose the Plaintiff's and Class Members' Private Information to unauthorized third parties;

c. whether Defendants had duties not to use Plaintiff's and Class Members' Private Information for non-healthcare purposes;

d. whether Defendants had duties not to use Plaintiff's and Class Members' Private Information for unauthorized purposes;

e. whether Defendants failed to adequately safeguard Plaintiff's and Class Members' Private Information;

f. whether and when Defendants actually learned of the Disclosure;

g. whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

h. whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

i. whether Defendants failed to properly implement and configure the tracking software on its Online Platforms to prevent the disclosure of confidential communications and Private Information;

j. whether Defendants adequately addressed and fixed the vulnerabilities that permitted the Disclosure to occur; and

k. whether Defendants engaged in unfair, unlawful, or deceptive practices by misrepresenting that they would safeguard Plaintiff's and Class Members' Private Information.

140. Typicality: Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendants' use and incorporation of Meta Pixel and other tracking technology.

141. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly, and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

142. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the

Class Members and the infringement of the rights and the damages Plaintiff has suffered is typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

143. Superiority and Manageability: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

144. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged. If the class action device were not used, Defendants would necessarily gain an unconscionable advantage because they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources. Moreover, the costs of individual suits could unreasonably consume the amounts that would be recovered, whereas proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged. Finally, individual actions would create a risk of inconsistent results and would be unnecessary and

duplicative of this litigation.

145. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

146. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

147. Unless a Class-wide injunction is issued, Defendants may continue in their unlawful disclosure and failure to properly secure the Private Information of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding Disclosure, and Defendants may continue to act unlawfully as set forth in this Complaint.

148. Further, Defendants have acted or refused to act on grounds generally applicable to the Class, and, accordingly, final injunctive or corresponding declaratory relief regarding the whole of the Class is appropriate.

149. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

a. whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. whether Defendants breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. whether Defendants failed to comply with their own Privacy Policy and applicable laws, regulations, and industry standards relating to the disclosure of patient information;

d. whether an implied contract existed between Defendants on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. whether Defendants breached the implied contract;

f. whether Defendants adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Disclosure;

h. whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information; and

i. whether Plaintiff and the Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

150. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

151. Defendants owed to Plaintiff and Class Members a duty to exercise reasonable care in handling and using Plaintiff's and Class Members' Private Information in their care and custody, including implementing industry-standard privacy procedures sufficient to reasonably protect the information from the disclosure and unauthorized transmittal and use of Private Information that

occurred.

152. Defendants acted with wanton and reckless disregard for the privacy and confidentiality of Plaintiff's and Class Members' Private Information by disclosing and providing access to this information to third parties for the financial benefit of the third parties and Defendant.

153. Defendants owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' disclosure of their Private Information to benefit third parties and Defendant. Defendants actively sought and obtained Plaintiff's and Class Members' Private Information.

154. Private Information is highly valuable, and Defendants knew, or should have known, the harm that would be inflicted on Plaintiff and Class Members by disclosing their Private Information to third parties. This disclosure was of benefit to third parties and Defendants by way of data harvesting, advertising, and increased sales.

155. Defendants breached their duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the personal information and Private Information of Plaintiff and Class Members. This failure actually and proximately caused Plaintiff's and Class Members' injuries.

156. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, inappropriate advertisements and use of their Private Information for advertising purposes, and increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

157. Defendants' breach of their common-law duties to exercise reasonable care and

their failures and negligence actually and proximately caused Plaintiff's and Class Members' actual, tangible, injury-in-fact and damages, including, without limitation, the unauthorized access of their Private Information by third parties, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of use of their information that resulted from and were caused by Defendants' negligence. These injuries are ongoing, imminent, immediate, and continuing.

COUNT II
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

158. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

159. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendants via their Website and Online Platforms.

160. Plaintiff and Class Members communicated sensitive PHI and PII—Private Information—that they intended for only Defendants to receive and that they understood Defendants would keep private.

161. Defendants' disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiff and Class Members is an intentional intrusion on Plaintiff's and Class Members' solitude or seclusion and their private affairs and concerns.

162. Plaintiff and Class Members had a reasonable expectation of privacy given Defendants' representations in their privacy policy. Moreover, Plaintiff and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential. Defendants' disclosure of PHI coupled with PII is highly offensive to the reasonable person.

163. As a result of Defendants' actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

164. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendants' invasion of their privacy and are entitled to just compensation, including monetary damages.

165. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as a result of their intrusions upon Plaintiff's and Class Members' privacy.

166. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendants' actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendants from engaging in such conduct in the future.

167. Plaintiff also seeks such other relief as the Court may deem just and proper.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)

168. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

169. As a condition of receiving medical care from Defendant, Plaintiff and the Class provided their Private Information and paid compensation for the treatment received. In so doing, Plaintiff and the Class entered into contracts with Defendants by which Defendants agreed to safeguard and protect such information, in their Privacy Policy and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

170. Implicit in the agreement between SIH and its patients, Plaintiff and the proposed Class Members, was the obligation that both parties would maintain the Private Information confidentially and securely.

171. SIH had an implied duty of good faith to ensure that the Private Information of Plaintiff and Class Members in its possession was only used only as authorized, such as to provide medical treatment, billing, and other medical benefits from SIH.

172. SIH had an implied duty to protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses.

173. Additionally, SIH implicitly promised to retain this Private Information only under conditions that kept such information secure and confidential.

174. Plaintiff and Class Members fully performed their obligations under the implied contract with SIH. SIH did not. Plaintiff and Class Members would not have provided their confidential Private Information to SIH in the absence of their implied contracts with SIH and would have instead retained the opportunity to control their Private Information for uses other than receiving medical treatment from SIH.

175. SIH breached the implied contracts with Plaintiff and Class members by disclosing Plaintiff's and Class Members' Private Information to an unauthorized third party.

176. SIH's acts and omissions have materially affected the intended purpose of the implied contracts requiring Plaintiff and Class Members to provide their Private Information in exchange for medical treatment and benefits.

177. As a direct and proximate result of Defendants' above-described breach of contract, Plaintiff and the Class have suffered (and will continue to suffer) the compromise and

disclosure of their Private Information and identities.

178. As a direct and proximate result of Defendants' above-described breach of contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

179. Plaintiff re-alleges and incorporates the preceding paragraphs of this Complaint as if fully set forth herein.

180. This claim is pleaded solely in the alternative to Plaintiff's Breach of Implied Contract claim.

181. Plaintiff and Class members conferred a monetary benefit upon SIH in the form of valuable sensitive medical information that Defendants collected from Plaintiff and Class Members under the guise of keeping this information private. Defendants collected, used, and disclosed this information for its own gain, including for advertisement purposes, sale, or trade for valuable services from third parties. Additionally, Plaintiff and the Class Members conferred a benefit on Defendants in the form of monetary compensation.

182. Plaintiff and Class Members would not have used SIH's services or would have paid less for those services, if they had known that Defendants would collect, use, and disclose their Private Information to third parties.

183. SIH appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class members.

184. As a result of SIH's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those

purchases without unreasonable data privacy and security practices and procedures that they received.

185. The benefits that Defendants derived from Plaintiff and Class Members rightly belong to Plaintiff and Class Members themselves. It would be inequitable under unjust enrichment principles for Defendants to be permitted to retain any of the profit or other benefits they derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

186. SIH should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds it received as a result of its conduct and the Disclosure alleged herein.

COUNT V
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

187. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

188. A relationship existed between Plaintiff and the Class, on the one hand, and Defendant, on the other, in which Plaintiff and the Class put their trust in Defendants to protect the Private Information of Plaintiff and the Class, and Defendants accepted that trust.

189. Defendants breached the fiduciary duty that they owed to Plaintiff and the Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect, and intentionally disclosing, their Private Information.

190. Defendants' breach of fiduciary duty was a legal cause of injury-in-fact and damage to Plaintiff and the Class.

191. But for Defendants' breach of fiduciary duty, the injury-in-fact and damage to

Plaintiff and the Class would not have occurred.

192. Defendants' breach of fiduciary duty contributed substantially to producing the damage to the Plaintiff and the Class.

193. As a direct and proximate result of Defendants' breach of fiduciary duty, Plaintiff and Class Members are entitled to and do demand actual, consequential, and nominal damages, injunctive relief, and all other relief allowed by law.

COUNT V
VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE PRACTICES ACT, 815 Ill. Comp. Stat. § 505/1 *et seq.*
(On Behalf of Plaintiffs and the Class)

194. Plaintiff re-alleges and incorporates the preceding paragraphs of this Complaint as if fully set forth herein.

195. The Illinois Consumer Fraud and Deceptive Practices Act ("CFDPA") makes it unlawful to employ "[u]nfair methods of competitions and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, or the use or employment of any practice described in [this section] . . . in the conduct of any trade or commerce." 815 Ill. Comp. Stat. Ann. 505/2.

196. Defendants were engaged "in the conduct of trade or commerce" by hosting and publishing their Website that they encouraged their patients to use and where they advertised their healthcare services to the public. *Id.*

197. SIH used unfair and deceptive acts or practices in the conduct of trade or commerce, including but not limited to the following.

a. Defendants encouraged their patients to use their Website and Online Platforms

while representing their commitment to protecting the privacy of their Personal Information. Meanwhile, Defendants shared Plaintiff and Class Members' Private Information with Facebook and possible others, without Plaintiff and Class Members' knowledge or consent.

b. Defendants promised that they would not use Plaintiff and Class Members' PHI to send them marketing information prior to obtaining their written permission. At the same time, Defendants knowingly collected Plaintiff's and Class Members' private information for marketing purposes. On information and belief, Defendants then used this information to market their services to Plaintiff and Class Members and thereby increase their profits.

c. Plaintiff and Class Members relied on SIH's representations in using SIH's Online Platform and thought they were communicating only with their trusted healthcare provider. In actuality, Defendants were surreptitiously intercepting and transmitting Plaintiff's and Class Member's communications from Plaintiff's and Class Members' browsers directly to Facebook.

198. SIH's Disclosure of Plaintiff and Class Members' Private Information was willful, knowing, and done with intent that Plaintiff and Class Members rely upon the concealment, suppression or omission of a material fact: that SIH was tracking Plaintiff's and Class Members' Private Information, using it for advertising purposes without their permission, and disclosing that information to unauthorized third parties.

199. The CFDPA provides that "[a]ny person who suffers actual damage as a result of a violation of this Act committed by any other person may bring an action against such person. The court, in its discretion may award actual economic damages or any other relief which the court

deems proper." 815 Ill. Comp. Stat. Ann. 505/10a(a). Further, "the Court may grant injunctive relief where appropriate and may award, in addition to the relief provided in this Section, reasonable attorney's fees and costs to the prevailing party." *Id.* at 505/10a(b).

200. Had Plaintiffs and members of the Classes been aware that their Private Information would be transmitted to unauthorized third parties, they would not have entered into such transactions and would not have provided payment or confidential medical information to SIH.

201. As a direct and proximate result of Defendants' unfair and deceptive acts and practices in violation of the DCSA, Plaintiff and Class Members have suffered damages for which Defendants are liable, including, but not limited to, the following.

a. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private.

b. Defendants eroded the essential confidential nature of the doctor-patient relationship.

c. Defendants took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value.

d. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendants' duty to maintain confidentiality.

e. Defendants' actions diminished the value of Plaintiffs' and Class Members' personal information.

202. Plaintiff and Class Members seek actual damages plus interest on damages at the legal rate, as well as all other just and proper relief afforded by the DCSA. As redress for

Defendants' repeated and ongoing violations, Plaintiff and Class Members are entitled to, *inter alia*, actual damages, reasonable attorneys' fees and costs, and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Mr. Doe, Individually, and on behalf of all others similarly situated, prays for judgment as follows:

A. for an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and Plaintiff's counsel as Class Counsel;

B. for equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. for equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity the type of Private Information compromised and unlawfully disclosed to third parties;

D. for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

E. ordering Defendants to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

F. for an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. for an award of punitive damages, as allowable by law;

H. for an award of reasonable attorneys' fees and costs under the CFDPA, the

common fund doctrine, and any other applicable law;

I. costs and any other expenses, including expert witness fees incurred by Plaintiff in connection with this action;

J. pre- and post-judgment interest on any amounts awarded; and

K. such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, pursuant to 735 Illinois Compiled Statutes 5/2-1105, hereby demands a trial by jury on all issues so triable.

Dated: June 15, 2023

Respectfully submitted,

By: /s/David Cates

David Cates, #6289198
Katie E. St. John, #6340448
THE CATES LAW FIRM, LLC
216 West Pointe Drive, Suite A
Swansea, IL 62226
Telephone: (618) 277-3644
Facsimile: (618) 277-7882
Email: dcates@cateslaw.com
kstjohn@cateslaw.com

Lynn A. Toops (No. 26386-49)
Mary Kate Dugan (No. 37623-49)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
mdugan@cohenandmalad.com

J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
Andrew E. Mize (*Pro Hac Vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)

gstranch@stranchlaw.com
amize@stranchlaw.com

Samuel J. Strauss (*Pro Hac Vice* forthcoming)
Raina Borelli (*Pro Hac Vice* forthcoming)
TURKE & STRAUSS, LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
(608) 237-1775
(608) 509-4423 (facsimile)
sam@turkestrauss.com
raina@turkestrauss.com

Counsel for Plaintiff and the Proposed Class

EXHIBIT A

Privacy Policy

Who We Are

This Notice describes the privacy practices of Southern Illinois Healthcare. It also applies to independent health care providers while providing services in our facilities, such as physicians, who are not employed by us but who attend patients in our facilities. This Notice, however, does not govern the privacy practices of these other health care providers for services they provide outside of our facilities.

Our Privacy Obligations

We are required by law to maintain the privacy and security of your individually identifiable health information **Protected Health Information**, or **("PHI")**, and to provide you with this Notice of our legal duties and privacy practices with respect to your Protected Health Information. PHI is individually identifiable under HIPAA if it includes your name, address, zip code, geographical codes, dates of birth, other elements of dates, telephone or fax numbers, email address, social security number, insurance information, medical record number, member or account number, certificate/license number, voice or finger prints, photos or any other unique identifying numbers, characteristics or codes of you. When we use or disclose your PHI, we are required to abide by the terms of this Notice (or other notice in effect at the time of the use or disclosure).

How We Typically Use Or Share Your Health Information Without Your Written Authorization

In certain situations, which we will describe in Section IV below, we must obtain your written authorization in order to use and/or disclose your PHI. However, we do not need any type of authorization from you for the following uses and disclosures:

Treatment. We can use your protected health information and share it with other healthcare professionals so we can treat and provide health care related services to you--for example, to diagnose and treat your injury or illness. In addition, we may contact you to provide appointment reminders or other health-related benefits and services that may be of interest to you.

Payment. We can use and share your protected health information to bill and get payment for the services that you received from us or our healthcare team; for example, to send your insurance a bill so they can pay us for the services we provided to you. We may also use and share your information to a third party who provides collection services on behalf of Southern Illinois Healthcare.

Health Care Operations. We can use and share your protected health information for our health care operations, which include various activities that improve the quality and cost effectiveness of the care that we deliver to you. For example, we may use and share your protected health information, such as your e-mail address, to contact you through a survey to ask your opinion about the quality of the services we provided to you.

Use or Disclosure for Directory of Individuals in one of Southern Illinois Healthcare's facilities. We may include your name, your location in the Southern Illinois Healthcare system, general health condition and religious affiliation in a patient directory. If you do not object, information in the directory can be shared to anyone who asks for you by name. Religious affiliation will only be shared to members of the clergy.

Disclosure to Relatives, Close Friends and Other Caregivers. We may use and share your protected health information to a family member, other relative, a close personal friend or any other person identified by you, if we
1) obtain your agreement; 2) provide you with the opportunity to object to the disclosure and you do not object.

If you are not present, or the opportunity to agree or object to a use or sharing of your protected health information cannot practicably be provided because of your incapacity or an emergency circumstance, we may exercise our professional judgment to determine whether sharing your information to a family member, other relative or close personal friend is in your best interest. We may also share your protected health information in order to notify (or assist in notifying) such persons of your location, general condition or death.

Fundraising Communications. We may contact you to request a tax deductible contribution to support important activities of Southern Illinois Healthcare. In connection with any fundraising, we may only share to our fundraising staff demographic protected health information about you (e.g., your name, address, phone number, age and gender), dates on which we provided health care to you, the department that treated you, the names of your treating physicians, and information regarding the outcome of your treatment and your health insurance status.

Public Health Activities. We may share your protected health information for the following public health activities: 1) to report health information to public health authorities for the purpose of preventing or controlling disease, injury or disability; 2) to report child abuse and neglect to government authorities authorized by law to receive such reports; 3) to report information about products and services to the U.S. Food and Drug Administration; 4) to alert a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition; and 5) to report information to your employer as required under laws involving work-related illnesses and injuries or workplace medical surveillance.

Victims of Abuse, Neglect or Domestic Violence. If we reasonably believe you are a victim of abuse, neglect or domestic violence, we can share your protected health information to a governmental authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence.

Health Oversight Activities. We can share your protected health information to a health oversight agency for ensuring compliance with the rules of government health programs such as Medicare or Medicaid.

Judicial and Administrative Proceedings. We can share your protected health information in response to a court or administrative order, or in response to a subpoena.

Law Enforcement Officials. We can share your protected health information to the police or other law enforcement officials as required or permitted by law or in compliance with a court order or subpoena.

Decedents. We can share protected health information to a coroner, medical examiner or funeral director when an individual dies.

Organ and Tissue Procurement. We can share your protected health information to organizations that facilitate organ, eye or tissue procurement.

Research. We can use or share your protected health information without your consent or authorization if our Institutional Review Board approves a waiver of authorization for disclosure.

Health or Safety. We can use or share your protected health information to prevent or lessen a serious and imminent threat to a person's or the public's health or safety.

Specialized Government Functions. We can use and share your protected health information to units of the government with special functions, such as the U.S. military or the U.S. Department of State under certain circumstances.

Workers' Compensation. We can share your protected health information relating to workers' compensation claims.

As required by law. We can use and share your protected health information when required to do so by any other law not already referred to in the preceding categories.

We may use and share your PHI without your consent or authorization to the Southern Illinois Health Information Exchange (SI HIE). A Health Information Exchange, or HIE, is a way of electronically sharing your health information to healthcare providers involved in your care. The purpose of the HIE is to give participating providers faster access to your health information that will facilitate safer, more timely, and efficient patient-centered care. For example, if you have an emergency and seek treatment at a Southern Illinois Healthcare hospital Emergency Department, the Emergency Department provider may have access to your electronic health information from your primary care provider.
If you do not want your health information maintained by Southern Illinois Healthcare to be accessible to authorized health care providers through the HIE, you may opt out by completing and sending a non-participation (opt-out) form to the Privacy Officer. If you decide to opt-out of the HIE, doctors, nurses and other healthcare providers will not be able to obtain and use your health information in the HIE when providing treatment to you. For further information about SI HIE and/or to obtain an opt-out form please visit www.sih.net or contact the Privacy Officer at the address found in Section VII.

Uses and Disclosures Requiring Your Written Authorization

Use or Disclosure with Your Authorization. For any purpose other than the ones described above in Section III, we can only use or share your protected health information when you grant us your written authorization. For instance, you will need to complete an authorization form before we can send your protected health information to your life insurance company or to an attorney.

Marketing. We must get your written permission prior to using your protected health information to send you any marketing materials. We can, however, without your permission 1) provide you with marketing materials in a face-to-face encounter; 2) give you a promotional gift of nominal value; 3) provide refill reminders or communicate with you about a drug or biologic that is currently prescribed to you; 4) communicate with you about products or services relating to your treatment, case management or care coordination.

Sale of Protection Health Information. We will not sell your protected health information without your written permission.

Uses and Disclosures of Your Highly Confidential Information. In addition, federal and Illinois law requires special privacy protections for certain highly confidential information, such as: 1) psychotherapy notes; 2) mental health and developmental disabilities services; 3) alcohol and drug abuse prevention, treatment and referral; 4) t HIV/AIDS testing, diagnosis or treatment; 5) venereal disease(s); 6) genetic testing; 7) child abuse and neglect; 8) domestic abuse of an adult with a disability; or 9) sexual assault. In order for us to share your highly confidential information for a purpose other than those permitted by law, we must obtain your written permission.

Your Rights Regarding Your Protected Health Information

Filing a Complaint. If you feel we have violated your privacy rights. You may contact our Privacy Officer. You may also file a complaint with the Director, Office for Civil Rights of the U.S. Department of Health and Human Services, 200 Independence Avenue, S.W. Washington, D.C. 20201, calling 1-877-6966775

or visiting the www.hhs.gov/hipaa/complaints or you can contact the Privacy Officer for contact information. We will not retaliate against you if you file a complaint.

Right to Request Additional Restrictions. You can ask us not to use or share certain health information for treatment, payment and health care operations. While we will consider all requests for additional restrictions carefully, we are not required to agree to a requested restriction. We are required to say "yes" if you ask us to restrict sharing your protected health information to 1) a health plan for purpose of carrying out payment or health operations; and 2) the PHI pertains solely to a healthcare item or service which has been fully paid out of pocket. If you wish to request additional restrictions, contact our Privacy Officer.

Right to Receive Confidential Communications. You can ask us to contact you in a specific way (for example, home or office phone or by mail to a specific address), we will say "yes" to all reasonable requests.

Right to Revoke Your Authorization. You may revoke Your Authorization, except to the extent that we have taken action in reliance upon it, by providing a written revocation statement to the Privacy Officer. A form of Written Revocation is available upon request from the Privacy Officer.

Right to Inspect and Copy Your Health Information. You can ask to see or get an electronic or paper copy of your medical record, billing record and other health information we have about you. We will provide a copy or a summary of your health information, usually within 30 days of your request. We may charge a reasonable, cost based fee. Under limited circumstances, we may deny you access to a portion of your records. To obtain information about viewing or getting a copy of your protected health information, visit www.sih.net, or contact the Health Information Department at the facility where you were a patient.

Right to Amend Your Records. You can ask us to correct protected health information about you that is maintained in your medical record or billing record that you think is incorrect or incomplete. To request an amendment to your records, visit www.sih.net, or contact the Health Information Department at the facility where you were a patient. We may say "no" to your request if we believe that the information that would be amended is accurate and complete. If we say "no" to your request you have the right to appeal our decision. You will receive our response to your request for a correction to your protected health information in writing and within 60 days.

Right to Receive An Accounting of Disclosures. You can ask for a list (accounting) of the times we've shared your health information without your authorization for six years prior to the date you ask The accounting list will provide who we shared your health information with and why. We will provide one accounting list a year for free but will charge a reasonable, cost based fee if you ask for another one within 12 months.

Breach Notification. We will let you know if a breach occurs that may have compromised the privacy or security of your information.

Right to Receive Paper Copy of this Notice. You can ask for a paper copy of this Notice at any time, even if you have agreed to receive the notice electronically.

Right to a Personal Representative. If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information. We will make sure the person has the authority and can act for you before we take any action.

Effective Date and Duration of This Notice

Effective Date. This Notice is effective on April 14, 2003.

Right to Change Terms of this Notice. We can change the terms of this Notice, and the changes will apply to all information we have about you. If we change this Notice, we will post the new notice in waiting areas around Southern Illinois Healthcare and on our Internet site at WWW.SIH.NET. You also may obtain any new notice by contacting the Privacy Officer.

Contact Information for Privacy Officer

You may contact the Privacy Officer at: Southern Illinois Healthcare, P. O. Box 3988, Carbondale, IL 62901. Telephone Number: 800-228-2631

Last Revised by Southern Illinois Healthcare 9/1/16